**Technical Brief**

# Protect Data in Motion with Seamless Email Encryption

March 2010

## NEED FOR EMAIL ENCRYPTION AT ITS PEAK

Because email has become the most prevalent tool for communication and collaboration by businesses and government, it has never been more vital to protect the flow of confidential private and company information transmitted via this medium. In the millions of messages sent weekly, content (including attachments) inevitably contains data that is private. In every organization, HR, finance, legal, executives, and other critical functions send email that is confidential at a minimum.

Based on the growing volumes of confidential and sensitive information traversing networks on a daily basis, regulatory bodies and business executives have turned their concerns to ensuring messaging is protected from unauthorized viewing. Regulations such as Sarbanes-Oxley, PCI, HIPAA, GLBA and others have been introduced to mandate that email messages containing sensitive or confidential data are handled securely.

With the increasing reliance on email, email encryption has emerged as a vital aspect of an overall email security solution to secure confidential data and yet continue to allow the free flow of email communications between colleagues, customers, and partners.

## THE SOLUTION: SEAMLESS EMAIL ENCRYPTION FROM WATCHGUARD®

WatchGuard Email Encryption technology, powered by Cisco, provides easy-to-use, business-class encryption to enable organizations to securely transmit and receive private and sensitive information. The WatchGuard Email Encryption solution is available with all WatchGuard XCS appliances, and is tightly integrated to enable instant-on security for confidential, regulated, and business-prudent information. It is an effective tool for organizations that require messaging security for privacy and compliance and yet also seek a solution with business-class features of reliable read receipts, secure replying and forwarding, message expiration, and message recalling.

The transparent nature of the WatchGuard Email Encryption solution lends to its ease of use. The WatchGuard XCS Data Loss Prevention engine identifies outgoing messages that meet pre-defined policies for confidentiality and automatically encrypt the messages with no special action required by the sender.

Encrypted messages are sent as HTML attachments to ordinary email messages and are directly delivered to the recipient who can decode and view the encrypted messages using any web browser. Users and administrators are able to view the status of individual encrypted messages and monitor the effectiveness of corporate confidentiality policies with features including detailed delivery, response tracking, and comprehensive message activity reporting.

WatchGuard Email Encryption enables organizations to:

- **Secure Confidential Information.** Outgoing messages containing sensitive information are transparently encrypted, delivered to any mailbox, and are easy for recipients to decrypt and view.
- **Adhere to Privacy and Compliance Regulations**. Sensitive messages are handled in compliance with industry regulations including HIPAA, PCI, SOX, GLBA and others without any effort on the part of the sender.
- **Enhance Control and Visibility.** Features such as guaranteed read receipts, message locking, and message expiration provide enterprise-class encryption.

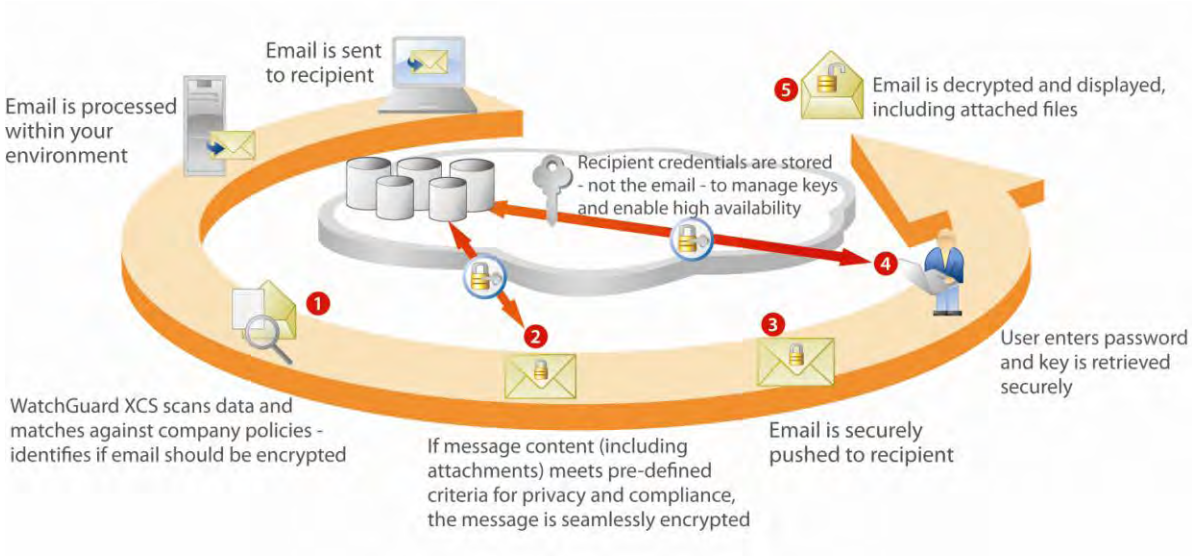
## THE WATCHGUARD EMAIL ENCRYPTION ARCHITECTURE

While en route from a sender to a recipient, an email message may pass through several waypoints and even multiple company networks before reaching its intended destination. Each of those waypoints and networks may have different security policies and settings. A single weak link along this path may compromise the confidential information within a message and can potentially result in leakage of sensitive information. The consequences could be detrimental, including:

- **Brand erosion**
- **Loss of customer confidence**
- **Financial repercussions**
- **Public embarrassment if it makes the headlines**

Encryption provides an extra layer of protection to ensure sensitive data is not seen by unwanted eyes. WatchGuard Email Encryption delivers an easy-to-use secure envelope solution which can be implemented for employees, customers, vendors, and other business partners. As shown in Figure 1 below, WatchGuard Email Encryption is an instant-on feature of the WatchGuard XCS.

**Figure 1: Instant-On Encryption**


Email is sent to recipient
Email is processed within your environment
5
Email is decrypted and displayed, including attached files
Recipient credentials are stored - not the email - to manage keys and enable high availability
4
1
2
3
User enters password and key is retrieved securely
WatchGuard XCS scans data and matches against company policies - identifies if email should be encrypted
If message content (including attachments) meets pre-defined criteria for privacy and compliance, the message is seamlessly encrypted
Email is securely pushed to recipient

All email sent from the organization passes through the WatchGuard XCS appliance Data Loss Prevention engine, which scans the data and matches it against pre-defined company and regulatory policies. Each message then undergoes remediation whereby it is checked to determine if it needs to be encrypted, quarantined, bounced, or handled in other ways as set by the policies set up by the Administrator, as shown in Figure 2 below.

Once undergoing content filtering inspection, if content or an attachment of a message matches a policy which has been specified for encryption, the WatchGuard XCS processes the outbound email and encrypts the message locally. The key used to encrypt the message is stored by Cisco Registered Envelope Service (CRES), while the message is queued for outbound delivery.

Recipients of encrypted messages using the WatchGuard Email Encryption solution do not require special software or applications to open an encrypted email. Encrypted messages can be opened with any email program and any web browser running on any operating system. The process is quite simple: recipients open an HTML email attachment, enter a password, and view the secure message.

**Figure 2: Discovery, Remediation and Inspection of Outgoing Messages**

## HOSTED KEYS SERVICE

WatchGuard Email Encryption uses the CRES hosted key service, thus enabling instant-on deployment and reduced management and hardware costs typically associated with local key servers. CRES technology provides the following benefits:

- Accounts are instantaneously created and users automatically enrolled
- User authentication and message key delivery
- Message tracking
- SecureReply capability for responding to encrypted messages

The CRES hosted key server only holds encryption keys and management information. It does not ever hold actual email messages and hence offers significant security benefits over other encryption solutions that host both messages and encryption keys on the same system.

## FILTERS AND LEXICONS FOR COMPLIANCE & POLICY MANAGEMENT

WatchGuard Email Encryption pulls on the capabilities of the WatchGuard XCS compliance and policy dictionaries or custom dictionaries created by the administrator, as well as policies that search the subject headers and body text of email messages as well as attachments, assisting organizations to comply with industry regulations including:

- **HIPAA** (Health Insurance Portability and Accountability Act)
- **GLBA** (Graham-Leach-Bliley Act)

- **SOX** (Sarbanes-Oxley Act)
- **European Privacy Initiative**
- **NASD 3010**
- **USA PATRIOT Act**
- **SEC Rule 17**

WatchGuard pre-defined compliance and privacy lexicons, which include terms, phrases, and alpha-numeric listings related to financial, health, and other private information assist enterprises to be compliant with industry regulations and alleviate the burdens and time required to set manual policies to identify sensitive information.

## FEATURES FOR ENHANCED VISIBILITY & CONTROL

Email security professionals using WatchGuard Email Encryption can expect to benefit from the exception control over business email, including:

**Guaranteed read receipts.** With traditional email, senders wishing to track read receipts must manually set up a read receipt request for each email prior to pressing the send button. Then, the sender must rely on the recipient to initiate a reply in order to receive a read receipt acknowledgment. WatchGuard Email Encryption eliminates this cumbersome process, since recipients must retrieve a decryption key from the system before they read its contents. As such, the system knows when the message has been read and provides automatic acknowledgement that the message has been retrieved. On the flip side, senders can be automatically notified by the system if an encrypted email has not been opened prior to expiry, alerting the sender to follow up directly with the recipient on important unread messages.

**Message Locking.** Occasionally, senders mistakenly send an encrypted email which contains inaccurate content, or is mistakenly sent to the wrong recipient, or quite simply contains information that needs to be recalled for various business reasons. With WatchGuard *Email* Encryption, senders can reduce the consequences of such an error by locking an encrypted message to prevent it from being viewed even after it has been delivered to the recipient's inbox.

**Message expiration.** Senders can set an expiration date for encrypted messages, after which they can no longer be opened. This can be done at the time the message is being sent, or the message can be expired manually at any time after the message has been delivered.

## ENCRYPTION OPTIONS: WatchGuard Email Encryption vs. Public Keys & Secure Webmail

WatchGuard Email Encryption is a next-generation solution that uses CRES secure envelope technology. It should not be confused with first-generation public key encryption solutions which require special software and certificates, or second-generation secure webmail encryption technologies, which uses a web server in the system to store encrypted email. Rather, WatchGuard Email Encryption uses a web browser to authenticate users and display decrypted messages. Ultimately, this results in a more cost-effective, secure, and efficient solution for securing email than public key or web-based systems. Key benefits of the WatchGuard Email Encryption solution include:

- **No Remote Message Storage.** Users need not be concerned about confidential messages being stored on a remote system – the encrypted incoming messages are delivered directly to the recipients' inboxes.
- **No Message Storage on Hosted Key Server**. The CRES hosted key server does not store messages. Encrypted messages and their keys are only ever combined on the recipient's computer. This results in a significantly more secure approach than storing both messages and decryption keys on a local server.

- **Unlimited Scalability.** Since WatchGuard Email Encryption leverages existing mail servers, there is no need to set up a new mail system. Costly scalability, bandwidth, deployment, and administration costs are hence eliminated.
- **No HTTPS Access Enablement Required.** WatchGuard Email Encryption does require inbound HTTPS access to be enabled for encrypted email retrieval.

## THE USER EXPERIENCE

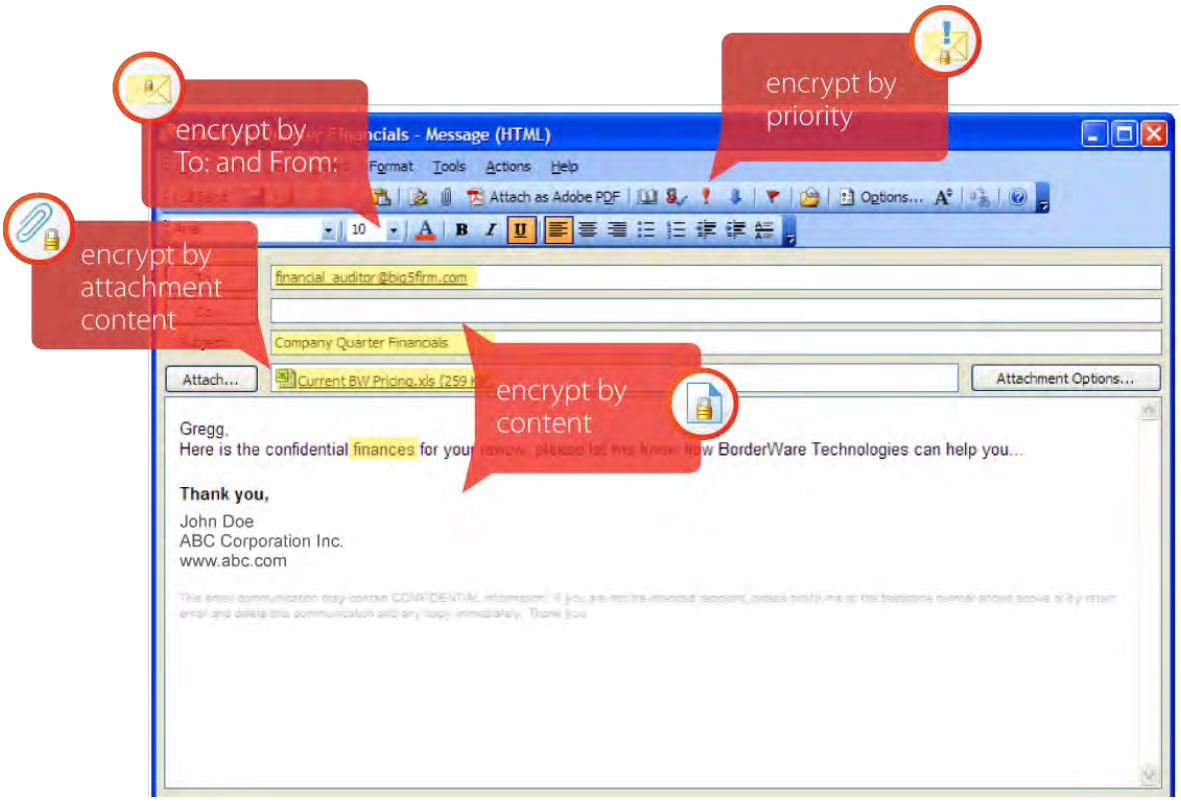
WatchGuard Email Encryption has been specifically designed with ease-of-use at the forefront such that employees, customers and other business partners can immediately appreciate the benefits associated with encrypted email communications.

**Sending Encrypted Email**

*Transparent Encryption*

WatchGuard Email Encryption is transparent to employees. When sending an encrypted email, the user simply composes and sends the email as he would at any other time. As shown in Figure 3 below, the content of the outgoing email is then automatically scanned and, if deemed to contain sensitive material as pre-defined by your organization's policies, it is then automatically encrypted.

**Figure 3: Transparent encryption based on pre-defined organizational policies**




*Manual Encryption*

WatchGuard Email Encryption also allows a sender to clearly flag a message for encryption by adding the word "Encrypt" in the subject line. This is then automatically identified by the system filter and the message is encrypted before being sent.

**Extending Encryption to Customers and Partners**

Once WatchGuard Email Encryption has been deployed internally, organizations can extend its benefits to customers and business partners who may wish to communicate with them in a confidential manner. WatchGuard Email Encryption allows secure communications between organizations and remote external users without the need to set up secure mailboxes before new users can send encrypted messages. It is a simple process. Links to WatchGuard Email Encryption can be added to an organization's public website. Those wishing to send secure communications merely click on the link and complete a simple registration process, at which time WatchGuard Email Encryption launches a browser-based message form. All the remote sender needs to do is then compose and send a message which is encrypted and forwarded to the intended recipient.

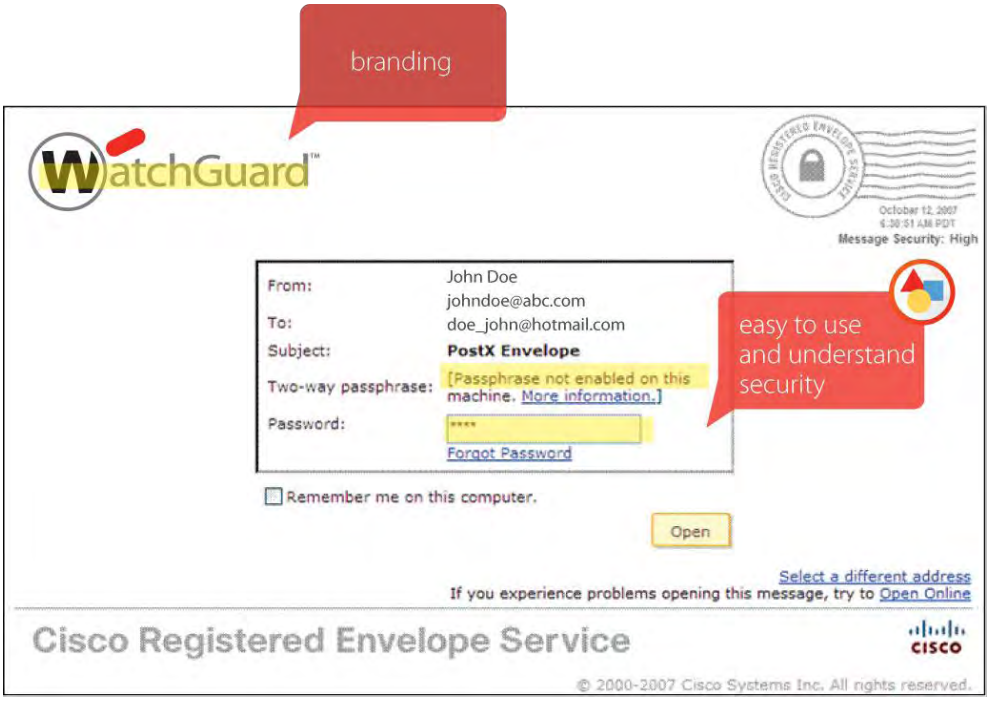
**Receiving Encrypted Email**

As mentioned previously, no special software is required to receive and read encrypted messages with WatchGuard Email Encryption. Recipients can open encrypted messages with any desktop email program or any web browser running on any operating system.

When receiving an encrypted email using WatchGuard Email Encryption, the recipient receives a notification message which arrives as a plain-text email with an HTML attachment. The notification envelope can be fully customizable with the sending organization's logo and branding, and supports both HTML and text.

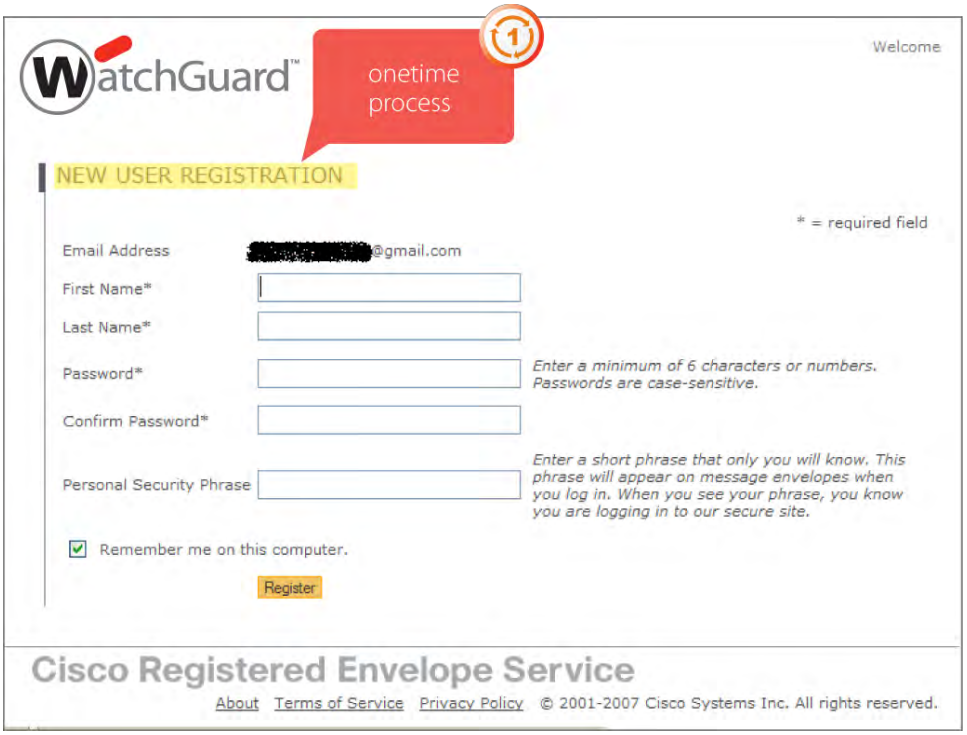
On opening the attachment, an envelope displays in the browser and asks the recipient for a password, as shown in Figure 4 below. Integrated anti-phishing through a two-way Personal Security Phrase (chosen by the user during account setup) enhances user confidence that the message is legitimate and has come from a trusted source.

**Figure 4: Recipient password-entry screen**



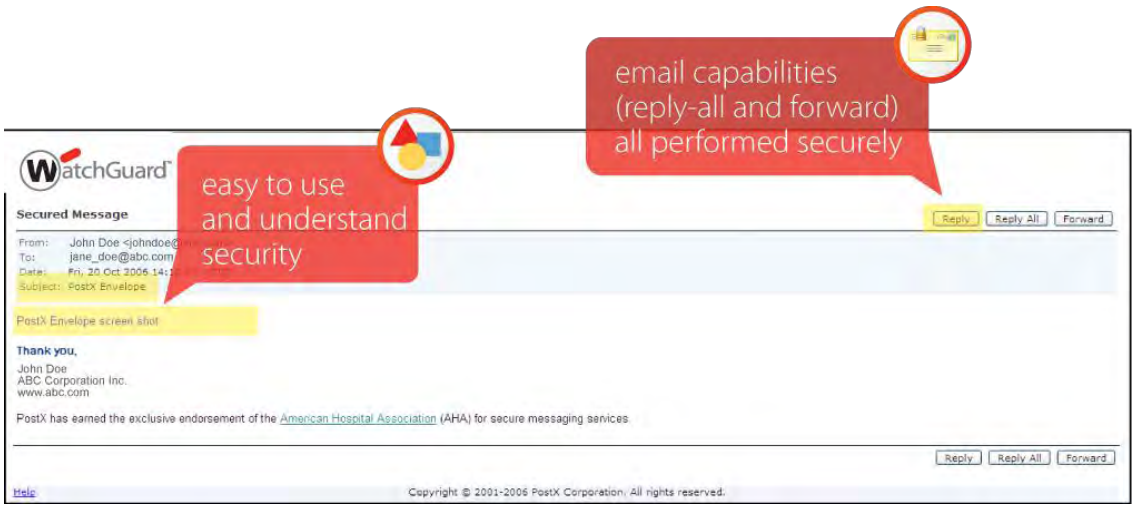
Those who are receiving encrypted emails for the first time are not required to set up an account in advance of using the system. Rather, they are directed to a screen, as shown in Figure 5, to create an account on CRES. The need for first-time user registration is automatically detected when no account exists for the recipient's email address. Once a recipient has set up an account on CRES, they can receive secure messages from any number of senders and can also log into their account at anytime to compose new encrypted messages.

**Figure 5: First-time recipient registration**


WatchGuard
onetime process
Welcome
NEW USER REGISTRATION
* = required field
Email Address
[redacted]@gmail.com
First Name*
Last Name*
Password*
Enter a minimum of 6 characters or numbers. Passwords are case-sensitive.
Confirm Password*
Enter a short phrase that only you will know. This phrase will appear on message envelopes when you log in. When you see your phrase, you know you are logging in to our secure site.
Personal Security Phrase
Remember me on this computer.
Register
Cisco Registered Envelope Service
About Terms of Service Privacy Policy © 2001-2007 Cisco Systems Inc. All rights reserved.

Once recipients have entered their passwords and the password has been successfully authenticated by CRES, the decryption key is sent to the recipient's system and the decrypted message is automatically displayed in the browser window, as shown in Figure 6.

**Figure 6: Decrypted message displayed in browser**



Once access to the decrypted message is obtained, the recipient has the ability to securely Reply, Reply All (configurable), and Forward (configurable), without requiring any special software.

WatchGuard Email Encryption provides enhanced security to keep unwanted eyes from viewing the document after it has been opened by requiring that the decryption key be retrieved from the server each time the message is read, allowing message to be locked by the sender even after they have been read.

**The Message Decoding Process**
Messages are encrypted using either AES or RC4 (both highly secure) industry standard algorithms. The HTML attachment in the notification contains the encrypted message content, as well as JavaScript to decrypt it locally, thus eliminating the need to install special software and enabling the solution to have universal reach with high usability.

In some cases, JavaScript is not always available. It may be stripped out at the receiving gateway or disabled in the recipient's browser. This does not hinder a recipient from easily decoding encrypted messages. CRES technology performs the encryption over a link secured with the SSL protocol. Once the recipient enters his or her valid password, the encrypted message is automatically posted to CRES for decryption. The decrypted message is then sent back to the recipient's browser for display. Although this method of decrypting messages is slower and less scalable than decoding them locally, it is a viable alternative when JavaScript is not available.

## ENCRYPTED MESSAGE TRACKING AND REPORTING

WatchGuard Email Encryption's web-based interface allows users and administrators to track messages and run reports on encrypted message activity, including:

**Delivery & Response Tracking**
When an encrypted message is opened, notifications are sent to the server and read receipts can be optionally generated for senders. Administrators can also configure time-based triggers to track when a message is opened and to signal when they have not been opened within a specified period of time.

**Message Activity Reporting**
WatchGuard XCS provides extensive content filtering reporting capabilities. Administrators can generate reports which indicate how many messages were flagged by each pre-defined policy and can also generate reports by user, as well.

## CONCLUSION

The WatchGuard Email Encryption solution is the most comprehensive and easy-to-use tool for keeping confidential information secure and avoiding embarrassing and potentially damaging and costly data leakage caused by user errors or oversights.

The WatchGuard Email Encryption solution provides maximum security to organizations and its users with its transparent encryption capabilities using custom or pre-defined policies, data loss prevention, and compliance dictionaries. Also, since messages are never stored on the same server as their keys, the WatchGuard Email Encryption solution ensures that only those with permission to view the encrypted message have access to its content.

Organizations concerned with compliance to both industry regulations and internal corporate policies can confidently rely on WatchGuard Email Encryption in correlation with the WatchGuard XCS to scan outbound messages with its powerful Data Loss Prevention and take the appropriate remediation, including blocking, quarantining, or automatically encrypting messages containing confidential and sensitive information in accordance with corporate policies. Using a policy-driven approach which can easily be extended and customized to meet individual needs for controlling confidential data, the WatchGuard Email Encryption

solution ensures that corporate rules and standards for sensitive information transmission are consistently applied.

Providing even greater control over business email are features such guaranteed read receipts, message locking, message expiration, and message tracking and reporting such that users and administrators have visibility into the status of encrypted message transmission and receipt.

No other solution on the market provides greater flexibility and ease-of-use. With its transparent application and universal reach, messages encrypted with WatchGuard Email Encryption can be sent to any email inbox without requiring administrators to set up new users or needing on the part of the recipient to install client software. Thus, confidential ad hoc communication with business partners and customers is simplified and scalable.

It has never been easier to deploy encryption as part of an overall email security solution. WatchGuard Email Encryption provides the necessary infrastructure so that all you have to do is enable it on the WatchGuard XCS, set Data Loss Prevention policies and compliance rules, and your outgoing emails and data will be protected from unintended viewers.

## NEXT STEPS

For more information on the powerful WatchGuard XCS family of extensible content security products with next-generation email encryption capabilities, visit www.watchguard.com/xcs.

**ADDRESS:**
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

**WEB:**
www.watchguard.com

**NORTH AMERICA SALES:**
+1.800.734.9905

**INTERNATIONAL SALES:**
+1.206.613.0895

**ABOUT WATCHGUARD**
Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. WatchGuard's award-winning extensible threat management (XTM) network security solutions combine firewall, VPN, and security services. The extensible content security (XCS) appliances offer content security across email and web, as well as data loss prevention. Both product lines help you meet regulatory compliance requirements including PCI DSS, HIPAA, SOX and GLBA. More than 15,000 partners represent WatchGuard in 120 countries. WatchGuard is headquartered in Seattle, Washington, with offices in North America, Latin America, Europe, and Asia Pacific. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. ©2010 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, and WatchGuard ReputationAuthority are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part.No. WGCE66694_031610